# Legacy Systems Sustainment Task Order PWS Template

**INSTRUCTIONS:**

1. **You must use this format for your NetCentric Legacy Systems Sustainment Performance Work Statement**

2. **Save a copy of this template and modify it according to your requirements. Each time a Legacy Systems Sustainment PWS is accomplished, make sure to download the newest version of the PWS template at the NETCENTS-2 websites. The language, standards, and references will be updated over time.**

3. **All bold italic text within brackets [ ] is instructional information specific to the section.**

4. **Text not within brackets is information that you are HIGHLY ENCOURAGED to keep in your PWS; only apply modifications, introduce additional information, or include updates in the event that standards or instructions change, or when deemed necessary by your specific program's or organization's policies.**

5. **Do not deviate from the format of this template. Doing so could delay the acquisition of your services and support. Using a standard template will help the offerors in knowing where to look for requirements and will decrease the time required to solicit proposals for the Task Orders.**

6. **All citations to policies, directives, instructions, and reference material are included in Section 8, *Applicable Standards & References*.**

7. **Before submitting your completed PWS, REMEMBER TO DELETE all instructional text contained within brackets. It is shown here for instructional purposes only and must not remain in the final document.**

# NETCENTS-2 SOLUTIONS
## Application Services – Full & Open / Small Business Companion
## Legacy Systems Sustainment
## Task Order Performance Work Statement (PWS)

| | |
|---|---|
| **Name:** | |
| **Organization:** | |
| **Address:** | ***[physical mailing address]*** |

## EXECUTIVE SUMMARY

**[*Provide a <u>short</u> description of the work to be performed*]**

# NETCENTS-2 Legacy Systems Sustainment Task Order PWS
## *[Requesting Agency Task Order Title]*

## 1. PURPOSE

***[In this paragraph, define the overall purpose and objectives of the Task Order]***

## 2. SCOPE

***[In this paragraph, summarize the specific type(s) of support your organization/program office is seeking and who the work supports – what organization(s) or domain(s). Do not go into too much detail, as this will be detailed under the "requirements" paragraphs that follow.]***

## 3. REQUIREMENT(S)/DESCRIPTION OF SERVICE(S)

***[In this paragraph, describe the broad level of service(s) required under the Task Order, not each specific task. It should be consistent with the outcomes defined in the Services Delivery Summary and linked to Air Force/organizational requirements. The objective is to state, using established industry/government standards, what we need (objective), not how we need each task accomplished (methodology). The following is a list of the service requirements supported by the Application Services ID/IQ contract. They can be modified as needed to meet Task Order requirement(s). To make your requirement(s) contractually binding the PWS must state, "The Contractor shall," for each requirement.]***

The operational environment, operational test environment, and independent test environment is assumed to be Government owned and managed, and the development environment is on contractor facilities, and associated hardware and software is Government-Off-The-Shelf (GOTS) with some Commercial-Off-The-Shelf (COTS) products embedded. Assume the contractor has access to the Governments help desk tracking system. The testing equipment and all hardware and software used at the contractor facility are assumed to be Government furnished. The system expects one major (baseline) release per year (releasing 100% of code), quarterly releases (modifying 10% of the code), and maintenance releases (modifying 15% of the code) to correct identified deficiencies. For the purpose of this evaluation, the defect rate is assumed to be zero. The following table provides system information that can be used to address technical and pricing sub-factors.

| **Factor** | **Data** |
|---|---|
| Code and data complexity | |
| Stability | |
| Number of concurrent users | |
| Application age | |
| Function Points Inputs | |

| Factor | Data |
|---|---|
| External Inputs | |
| External Outputs | |
| Logical Internal Files | |
| External Interfaces | |
| External Inquiries | |
| Initial response time | |
| Life expectancy | |
| Operating system | |
| Platform | |
| Programming Languages | |
| Programs | |
| Database | |
| COTS | |
| Avg transactions per day | |
| Interfaces | |
| Upgrades | |
| Average help desk call volume | |

### 3.1 Systems Support

The Contractor shall design, develop, test and package systems and software changes as well as provide problem resolutions for the existing system. The Contractor shall maintain the current baseline of the system and provide software change and problem fixes to these baselines as required. The Contractor shall provide to the Government all developed, modified, or converted source modules, processes, programs, scripts, operating instructions, databases, system files, documentation, test files and test conditions used to develop each approved systems change request. Specific tasks may include the following:

- Maintain existing legacy systems and environments IAW disciplined engineering practices and sustain applications, databases, and interfaces in compliance with applicable AF/DoD standards

- Conduct software development, software security, web services development, web services testing, smart phone or other IT device applications and testing, security layer integration, database clean-up, data wrapping, and data conversion

- Perform system performance tuning, system re-hosting, and integration services

- Migrate legacy systems to an Enterprise Resource Planning (ERP) system or an existing standard infrastructure such as the Global Combat Support System (GCSS) or DoD Enterprise Computing Center (DECC)

- Utilize Government-Off-The-Shelf (GOTS) or approved Commercial-Off-The-Shelf (COTS) tools for systems design and development

### 3.2 Help Desk Support

The Contractor shall provide continuous Help Desk Tier 1, Tier 2, and Tier 3 support 7-days a week, 365-days a year. The Contractor shall provide patch management support for multiple software versions, providing technical assistance, training, warranty, and maintenance, for reporting deficiencies in software and hardware. The Contractor shall provide methods for responding to customer requests and order processing. The Contractor shall use deficiency reporting tools and establish methods for resolving and closing deficiency reports. The Contractor shall monitor discrepancy reports, provide performance improvement recommendations, identify environmental changes and changes in Government equipment or regulations and make the recommended performance improvement, environmental, or equipment changes as requested by the Government.

Definitions:

- Tier 1 – Basic application software and/or hardware support

- Tier 2 – More complex support on application software and/or hardware

- Tier 3 – Usually subject matter experts, support on complex hardware and OS software issues

### 3.3 *[Next Requirement]*

## 4. ENGINEERING REQUIREMENTS

### 4.1 Systems Engineering

***[Insert additional MAJCOM or organization SEP policy, requirements or guidelines. Include any special SEP instruction for Top Secret/TS SCI systems or applications.]***

The contractor shall employ disciplined systems engineering processes including, but not limited to, requirements development, technical management and control, system/software design and architecture, integrated risk management, configuration management, data management, and test, evaluation, verification and validation practices throughout the period of performance of task orders in accordance with AFI 63-1201, *Life Cycle Systems Engineering*. If applicable, the contractor shall follow and refer to the Air Force Program Executive Office (AFPEO) Business

Enterprise Systems (BES) Systems Engineering Process (SEP) website for common plans, procedures, checklists, forms, and templates that support system life cycle management and systems engineering processes as it applies to Defense Acquisition, Technology, and Logistics tailored to Capability Maturity Model Integrated (CMMI) disciplines, or be able to demonstrate comparable processes and artifacts.

The contractor shall develop solutions that employ principles of open technology development and a modular open systems architecture for hardware and software as described in the DoD Open Technology Development Guidebook and Net-Centric Enterprise Solutions for Interoperability (NESI) body of knowledge. The contractor's systems engineering plan and design activities shall also adhere to the DoD Information Sharing and Net-Centric Strategies published by the DoD CIO, and the engineering body of knowledge and lessons-learned accumulated in NESI.

All services provided under this Task Order shall function and be in compliance with the Federal Desktop Core Configuration (FDCC), Information Assurance guidelines, and Security Technical Implementation Guides (STIGs) for systems and applications. Services for Top Secret and/or TS SCI systems and applications will be in compliance with standards, policies and guidelines identified in the task order.

### 4.2 Architecture and System Design

The contractor shall support the design and development of systems and applications and their integration into the overarching enterprise architecture. The contractor shall provide all required design and development documents, and supporting architectural documentation in compliance with Department of Defense Architectural Framework (DoDAF) Enterprise Architecture guidance, or other frameworks as identified in the task order.

### 4.3 Configuration Management

The contractor shall accomplish Configuration Management (CM) activities as described in the task order. CM activities include baseline identification, change control, status accounting, and auditing.

### 4.4 Testing

***[Insert additional test requirements for Top Secret/TS SCI systems or applications]***

The contractor shall conduct rapid testing and deployment of Core Data Services and Aggregation and Presentation Layer Services using distributed testing environments. The contractor shall develop dynamic testing environments to support C&A and functional testing. The contractor shall perform testing of Top Secret and/or TS SCI systems and applications IAW standards, policies and guidelines identified in the task order.

#### 4.4.1 Test Lab

When requested and specified in the task order, the contractor shall establish and maintain a system integrated test lab that is capable of supporting a full range of integration test activities for both the currently fielded system as well as maintenance/modernization releases. The currently fielded system includes the most current version and up to three previous versions for products that have not yet been declared 'end of life.' The contractor shall support test activities in areas which include, but are not limited to, product testing (regression testing and new capability testing), operational scenarios (real world simulation testing considering system

topology and concept of operation, disaster recovery, clustering, and load balancing), stress and longevity (throughput, speed of service, and duration), interoperability, security (VPN, Firewall, security configuration of products and operating systems, and CAC Middleware testing), usability, transition (upgrade paths), and packaging/installation.

### 4.4.2 Product/System Integration Testing

The contractor shall perform testing and inspections of all system services to ensure the technical adequacy and accuracy of all work, including reports and other documents required in support of that work. The contractor shall conduct on-site testing when requested. When specified by the Government, the contractor shall participate with the Government in testing the complete system or application which may include premise equipment, distribution systems or any additional telecommunications equipment or operating support systems identified in the task order. After appropriate corrective action has been taken, all tests including those previously completed related to the failed test and the corrective action shall be repeated and successfully completed prior to Government acceptance. Pre-cutover audits will consist of verification of all testing completed by the contractor such that the system is deemed ready for functional cutover. As part of this audit, any engineered changes or approved waivers applicable to the installation will be reviewed and agreed upon between the contractor and the Government. Post-cutover audits will verify that all post-cutover acceptance testing has been performed satisfactorily IAW the standard practices and identify those tests, if any, which have not been successfully completed and must be re-tested prior to acceptance. Testing shall be performed in two steps: operational testing, then system acceptance testing. The contractor shall provide a logical test process that minimizes interruptions and avoids sustained downtime and presents a contingency procedure to be implemented in the event of systems failure during testing.

### 4.4.3 Simulated Operational Testing

The contractor shall conduct testing ranging from data entry and display at the user level combined with system loading to represent a fully operational system. The contractor shall accomplish operational testing IAW the Government-approved test plan as specified in the task order. The plan shall consist of a program of tests, inspections and demonstrations to verify compliance with the requirements of this Task Order. The contractor shall document test results in the test report(s). The contractor shall furnish all test equipment and personnel required to conduct operational testing. During the installation/test phase, the Government reserves the right to perform any of the contractor performed inspections and tests to assure solutions conform to prescribed requirements. The contractor shall be responsible for documenting deficiencies and tracking them until they are resolved. The Government will not be expensed for correcting deficiencies that were the direct result of the contractor’s mistakes.

### 4.4.4 Acceptance Testing

The contractor shall provide on-site support during the acceptance-testing period. Acceptance testing shall be initiated upon acceptance of the operational test report and approval of the acceptance test plan. If a phased installation concept is approved in the Systems Installation Specification Plan (SISP), acceptance shall be based on the increments installed IAW the SISP. This on-site support shall be identified in the acceptance test plan.

### 4.4.5 System Performance Testing

***[Establish system or application availability and performance parameters, thresholds and/or incentives]***

The contractor shall provide system performance testing. The acceptance test will end when the system or application has maintained the site-specific availability rate specified in the task order. In the event the system or application does not meet the availability rate, the acceptance testing shall continue on a day-by-day basis until the availability rate is met. In the event the system or application has not met the availability rate after 60 calendar days, the Government reserves the right to require replacement of the component(s) adversely affecting the availability rate at no additional cost.

### 4.5 Information Assurance

***[Modify Information Assurance requirements as they relate to a system or application.]***

The contractor shall ensure that all system or application deliverables meet the requirements of DoD and AF Information Assurance (IA) policy. Furthermore, the contractor shall ensure that personnel performing IA activities obtain, and remain current with, required technical and/or management certifications.

#### 4.5.1 System IA

For those solutions that will not inherit existing network security controls, and thus integrate an entirely new application system consisting of a combination of hardware, firmware and software, system security assurance is required at all layers of the TCP/IP DoD Model. The contractor shall ensure that all system deliverables comply with DoD and AF IA policy, specifically DoDI 8500.2, *Information Assurance Implementation*, and AFI 33-200, *Information Assurance Management*. To ensure that IA policy is implemented correctly on systems, contractors shall ensure compliance with DoD and AF Certification & Accreditation policy, specifically DoDI 8510.01, *DoD Information Assurance Certification and Accreditation Process (DIACAP)*, and AFI 33-210, *Air Force Certification and Accreditation Process (AFCAP)*. The contractor shall also support activities and meet the requirements of DoDI 8520.02, *Public Key Infrastructure (PKI) and Public Key (PK) Enabling,* in order to achieve standardized, PKI-supported capabilities for biometrics, digital signatures, encryption, identification and authentication.

#### 4.5.2 Application IA

For those solutions that will be deployed to Infrastructure as a Service (IaaS), Platform as a Service (PaaS) or similar environments, and thus inherit existing network security controls, application security assurance is required at the Application layer of the TCP/IP DoD Model. The contractor shall ensure that all application deliverables adhere to Public Law 111-383, which states the general need for software assurance. Specifically, the contractor shall ensure that all application deliverables comply with Defense Information Systems Agency (DISA) Application Security Development Security Technical Implementation Guide (STIG), which includes the need for source code scanning to mitigate vulnerabilities associated with SQL injections, cross-site scripting, and buffer overflows. The contractor shall also support activities and meet the requirements of DoDI 8520.02, *Public Key Infrastructure (PKI) and Public Key (PK) Enabling*, in order to achieve standardized, PKI-supported capabilities for biometrics, digital signatures, encryption, identification and authentication.

#### 4.5.3 Personnel IA

Personnel performing Information Assurance (IA) activities are required to obtain, and remain current with, technical and/or management certifications to ensure compliance with DoD 8570.01-M, *Information Assurance Workforce Improvement Program*, 19 December 2005 (with

all current changes), and as stipulated in Section H, Clause H101 of the overarching Application Services RFP.

## 5. CONTRACTUAL REQUIREMENTS

***[This section is here to capture all the requirements that do not logically fit or are not specifically covered in any of the other sections. Modify as needed to meet your requirement. This section may include such things as required physical security, emergency or special events, environmental or hazardous requirements, security requirements, and specific training requirements. Modify each section IAW your requirements. Delete those that do not apply.]***

### 5.1 Contractors Use of NETCENTS-2 Products Contract

The contractor shall obtain all products and associated peripheral equipment required by each individual task order from the NETCENTS-2 Products contract as stipulated in Section H Clause H098 of the overarching Application Services RFP.

### 5.2 Place of Performance

***[The place of performance will be designated in each TO. Work shall be performed at either the customer (Government) or contractor site. Travel to other Government or contractor facilities may be required and will be specified in each TO. Exercise and deployment support will be identified in applicable TOs.]***

### 5.3 Normal Hours of Operation

***[Identify customer specific hours that are applicable to this Task Order, i.e. 7-4, 8-5, 24 x 7 x 365. Sample language is provided below.]***

The average workweek is 40 hours. The average workday is 8 hours and the window in which those 8 hours may be scheduled is between 6:00 AM and 6:00 PM, Monday through Friday or as specified in the TO, except for days listed in Clause G021, Contract Holidays, in the overarching ID/IQ contract. Billable hours are limited to the performance of services as defined in the TO. Government surveillance of contractor performance is required to give reasonable assurance that efficient methods and effective cost controls are being used. Work in excess of the standard 40 hour work week requires prior written approval by the Quality Assurance Personnel (QAP).

### 5.4 Government Furnished Property

***[Identify any GFE and/or GFI, and any limitations that will be provided to the contractor. For GFE, provide serial numbers and all identifying information. (Note: If GFE is a sizable list, indicate for example, "50 PC Pentium IVs," and state that serial numbers will be provided at Task Order award, along with location and delivery method.) For GFI, list by document number and title, date, etc. Include standards, specifications, and other reference material required to perform the Task Order. Include any facilities the Government may need to provide to contractor personnel for project performance. Sample language is provided below.]***

When the Task Order requires the contractor to work in a Government facility, the Government will furnish or make available working space, network access, and equipment to include:

- Windows PC with Microsoft Office Suite (Outlook, Word, Excel, PowerPoint, etc.)
- Telephone (local/long distance calls authorized as dictated by Task Order performance requirements)
- Facsimile
- Copier
- Printer

Copies of required Government furnished materials cited in the solicitation, PWS, DD Form 254, and/or in the Task Order will be provided to the contractor in hard copy or soft copy. All materials will remain the property of the Government and will be returned to the responsible Government QAP upon request or at the end of the Task Order period of performance.

Equipment purchased by the contractor with the approval of the Government and directly charged to this Task Order shall be considered government owned-contractor operated equipment. The contractor shall conduct a joint inventory and turn in this equipment to the COR upon request or completion of the Task Order.

### 5.5 Billable Hours

***[Modify as required for Task Order requirements. Sample language is provided below.]***

In order for man-hours to be billed, deliverable services must have been performed in direct support of a requirement in the TO PWS. In the course of business, situations may arise where Government facilities may not be available for performance of the TO requirements (i.e., base closure due to weather, Force Protection conditions, etc.). When the base is officially closed no contractor services will be provided and no charges will be incurred and/or billed to any TO. There may also be occasions when support contractors are invited to participate in morale and recreational activities (i.e., holiday parties, golf outings, sports days and other various social events). Contractor employees shall not be directed to attend such events by the Government. Since a contract employee is not a government employee, the contract employee cannot be granted the same duty time activities as Government employees. Participation in such events is not billable to the TO and contractor employee participation should be IAW the employees, company's policies and compensation system.

### 5.6 Non-Personal Services

***[Modify as required for Task Order requirements. Sample language is provided below.]***

The Government will neither supervise contractor employees nor control the method by which the contractor performs the required tasks. Under no circumstances shall the Government assign tasks to, or prepare work schedules for, individual contractor employees. It shall be the responsibility of the contractor to manage its employees and to guard against any actions that are of the nature of personal services, or give the perception of personal services. If the contractor feels that any actions constitute, or are perceived to constitute personal services, it shall be the contractor's responsibility to notify the Task Order (TO) Contracting Officers CO immediately. These services shall not be used to perform work of a policy/decision making or management nature, i.e., inherently Governmental functions. All decisions relative to programs supported by the contractor shall be the sole responsibility of the Government. These operating procedures may be superseded by Theater Commander's direction during deployments.

### 5.7 Contractor Identification

***[Modify as required for Task Order requirements. Sample language is provided below.]***

All contractor/subcontractor personnel shall be required to wear AF-approved or provided picture identification badges so as to distinguish themselves from Government employees. When conversing with Government personnel during business meetings, over the telephone or via electronic mail, contractor/subcontractor personnel shall identify themselves as such to avoid situations arising where sensitive topics might be better discussed solely between Government employees. Contractors/subcontractors shall identify themselves on any attendance sheet or any coordination documents they may review. Electronic mail signature blocks shall identify their company affiliation. Where practicable, contractor/subcontractors occupying collocated space with their Government program customer should identify their work space area with their name and company affiliation. ***Refer to Clause H063 of the overarching ID/IQ contract for specific guidance.***

### 5.8 Performance Reporting

The contractor's performance will be monitored by the Government and reported in Contractor Performance Assessment Reporting (CPARs). Performance standards shall include the contractor's ability to provide or satisfy the following:

- Provide quality products, incidentals, and customer support
- Meet customer's agreed-upon timelines for scheduled delivery of items, warranty, and/or incidental services: Emergency/critical, Maintenance/Warranty – 24 x 7 x 365, and remote OCONUS, OCONUS vs. CONUS response times
- Timely and accurate reports
- Responsive proposals
- Configuration assistance as identified in each delivery order

### 5.9 Program Management / Project Management

The contractor shall identify a Program Manager or a Project Manager who shall be the primary representative responsible for all work awarded under this task order, participating in Program/Project Management Reviews and ensuring all standards referenced herein are adhered to.

#### 5.9.1 Services Delivery Summary

***Reference Section 6,* Services Delivery Summary*, of this Task Order PWS for specific performance objectives.***

The contractor's performance at the contract level will be assessed quarterly by a process that measures success towards achieving defined performance objectives. The Services Delivery Summary will be in accordance with AFI 63-124, Performance Based Services Acquisition and FAR Subpart 37.6, Performance-Based Acquisition.

#### 5.9.2 Task Order Management

The contractor shall establish and provide a qualified workforce capable of performing the required tasks. The workforce may include a project/task order manager who will oversee all aspects of the task order. The contractor shall use key performance parameters to monitor work performance, measure results, ensure delivery of contracted product deliverables and solutions,

support management and decision-making and facilitate communications. The contractor shall identify risks, resolve problems and verify effectiveness of corrective actions. The contractor shall institute and maintain a process that ensures problems and action items discussed with the Government are tracked through resolution and shall provide timely status reporting. Results of contractor actions taken to improve performance shall be tracked, and lessons learned incorporated into applicable processes. The contractor shall establish and maintain a documented set of disciplined, mature, and continuously improving processes for administering all contract and Task Order efforts with an emphasis on cost-efficiency, schedule, performance, responsiveness, and consistently high-quality delivery. The contractor shall provide transition plans as required.

### 5.9.3 Documentation and Data Management

The contractor shall establish, maintain, and administer an integrated data management system for collection, control, publishing, and delivery of all program documents. The data management system shall include but not be limited to the following types of documents: CDRLs, White Papers, Status Reports, Audit Reports, Agendas, Presentation Materials, Minutes, Contract Letters, and Task Order Proposals. The contractor shall provide the Government with electronic access to this data, including access to printable reports.

### 5.9.4 Records, Files, and Documents

All physical records, files, documents, and work papers, provided and/or generated by the Government and/or generated for the Government in performance of this PWS, maintained by the contractor which are to be transferred or released to the Government or successor contractor, shall become and remain Government property and shall be maintained and disposed of IAW AFMAN 33-363, Management of Records; AFI 33-364, Records Disposition – Procedures and Responsibilities; the Federal Acquisition Regulation, and/or the Defense Federal Acquisition Regulation Supplement, as applicable. Nothing in this section alters the rights of the Government or the contractor with respect to patents, data rights, copyrights, or any other intellectual property or proprietary information as set forth in any other part of this PWS or the Application Services contract of which this PWS is a part (including all clauses that are or shall be included or incorporated by reference into that contract).

### 5.9.5 Security

Individuals performing work under these task orders shall comply with applicable program security requirements as stated in the task order. NETCENTS-2 will support the following levels of security: Unclassified; Unclassified, But Sensitive; Secret (S); Secret Sensitive Compartmented Information (S/SCI); Top Secret (TS); and Top Secret Sensitive Compartmented Information (TS/SCI).

Task orders may require personnel security clearances up to and including Top Secret, and may require all employees to be United States citizens. The security clearance requirements will depend on the security level required by the proposed task order. The task orders may also require access to sensitive compartmented information (SCI) for which SCI eligibility will be required. Contractors shall be able to obtain adequate security clearances prior to performing services under the task order. The Contract Security Classification Specification (DD Form 254) will be at the basic contract and task order level and will encompass all security requirements. All contractors located on military installations shall also comply with Operations Security (OPSEC) requirements as set forth in DoD Directive 5205.02, Operations Security Program and AFI 10-701, Operations Security. In accordance with DoD 5200.2-R, Personnel Security

Program (Jan 87), DoD military, civilian, consultants, and contractor personnel using unclassified automated information systems, including e-mail, shall have, at a minimum, a completed favorable National Agency Check plus Written Inquiries (NACI).

The types of Personnel Security Investigations (PSI) required for the contractor vary in scope of investigative effort depending upon requirements of the Government and/or conditions of the Task Order. In cases where access to systems such as e-mail is a requirement of the Government, application/cost for the PSI shall be the responsibility of the Government. In cases where access to systems is as a condition of the Task Order, application/cost for the appropriate PSI shall be the responsibility of the contractor. In such instances, the contractor shall diligently pursue obtaining the appropriate PSI for its employees prior to assigning them to work any active task order. Acquisition planning must consider Anti-Terrorism (AT) measures when the effort to be contracted could affect the security of operating forces (particularly in-transit forces), information systems and communications systems IAW DoD Instructions 2000.16 Anti Terrorism Standards.

#### 5.9.5.1 Transmission of Classified Material

The contractor shall transmit and deliver classified material/reports IAW the National Industrial Security Program Operating Manual (DoD 5220.22-M). These requirements shall be accomplished as specified in the Task/Delivery Order.

#### 5.9.5.2 Protection of System Data

***[Modify as required for Task Order requirements. Sample language is provided below.]***

Unless otherwise stated in the task order, the contractor shall protect system design-related documents and operational data whether in written form or in electronic form via a network in accordance with all applicable policies and procedures for such data, including DoD Regulation 5400.7-R and DoD Manual 5200.01(v1-v4) to include latest changes, and applicable service/agency/ combatant command policies and procedures. The contractor shall protect system design related documents and operational data at least to the level provided by Secure Sockets Layer (SSL)/Transport Security Layer (TSL)-protected web site connections with certificate and or user ID/password-based access controls. In either case, the certificates used by the Contractor for these protections shall be DoD or IC approved Public Key Infrastructure (PKI) certificates issued by a DoD or IC approved External Certification Authority (ECA) and shall make use of at least 128-bit encryption.

#### 5.9.5.3 System and Network Authorization Access Requests

***[Modify as required for Task Order requirements. Sample language is provided below.]***

For Contractor personnel who require access to DoD, DISA, or Air Force computing equipment or networks, the Contractor shall have the employee, prime or subcontracted, sign and submit a System Authorization Access Report (SAAR), DD Form 2875.

### 5.9.6 Travel

The contractor shall coordinate specific travel arrangements with the individual Contracting Officer or Contracting Officer's Representative to obtain advance, written approval for the travel about to be conducted. The contractor's request for travel shall be in writing and contain the dates, locations and estimated costs of the travel in accordance with the basic contract clause H047.

If any travel arrangements cause additional costs to the task order that exceed those previously negotiated, written approval by CO is required, prior to undertaking such travel. Costs associated with contractor travel shall be in accordance with FAR Part 31.205-46, Travel Costs. The contractor shall travel using the lower cost mode transportation commensurate with the mission requirements. When necessary to use air travel, the contractor shall use the tourist class, economy class, or similar accommodations to the extent they are available and commensurate with the mission requirements. Travel will be reimbursed on a cost reimbursable basis; no profit or fee will be paid.

### 5.9.7 Other Direct Cost (ODC)

The contractor shall identify ODC and miscellaneous items as specified in each task order. No profit or fee will be added; however, DCAA approved burden rates are authorized.

### 5.10 Training

Contractor personnel are required to possess the skills necessary to support their company's minimum requirements of the labor category under which they are performing. Training necessary to meet minimum requirements will not be paid for by the Government or charged to TOs by contractors.

### 5.10.1 Mission-Unique Training

In situations where the Government organization being supported requires some unique level of support because of program/mission-unique needs, then the contractor may directly charge the TO on a cost reimbursable basis. Unique training required for successful support must be specifically authorized by the TO CO. Labor expenses and travel related expenses may be allowed to be billed on a cost reimbursement basis. Tuition/Registration/Book fees (costs) may also be recoverable on a cost reimbursable basis if specifically authorized by the TO CO. The agency requiring the unique support must document the TO file with a signed memorandum that such contemplated labor, travel, and costs to be reimbursed by the Government are mission essential and in direct support of unique or special requirements to support the billing of such costs against the TO.

### 5.10.2 Other Government-Provided Training

The contractor's employees may participate in other Government provided training, on a non-discriminatory basis as among contractors, under the following circumstances:

(1) The contractor employees' participation is on a space-available basis,

(2) The contractor employees' participation does not negatively impact performance of this task order,

(3) The Government incurs no additional cost in providing the training due to the contractor employees' participation, and

(4) Man-hours spent due to the contractor employees' participation in such training are not invoiced to the task order

### 5.11 Data Rights and Non-Commercial Computer Software

In order to implement the provisions at DFARS 252.227-7013(b) and (e) and DFARS 252.227-7014(b) and (e) and DFARS 252.227-7017, the Contractor shall disclose to the ordering

Contracting Officer and ordering office in any proposal for a task order, or after award of a task order if not previously disclosed in the proposal, any technical data or non-commercial computer software and computer software/source code documentation developed exclusively at government expense in performance of the task order. This disclosure shall be made whether or not an express requirement for the disclosure is included or not included in the PWS or solicitation for the order. The disclosure shall indicate the rights asserted in the technical data and non-commercial computer software by the Contractor and rights that would be acquired by the government if the data or non-commercial software was required to be delivered under the task order and its CDRL requirements and any cost/price associated with delivery. This disclosure requirement also applies to segregable routines of non-commercial software that may be developed exclusively at Government expense to integrate Commercial Software components or applications provided under a commercial software license or developed to enable Commercial Software to meet requirements of the Task Order. This disclosure obligation shall apply to technical data and non-commercial computer software developed exclusively at Government expense by subcontractors under any Task Order. Performance of this disclosure requirement shall be considered a material performance requirement of any task order under which such technical data or non-commercial computer software is developed exclusively at Government expense.

### 5.12 COTS Manuals and Supplemental Data

The contractor shall provide documentation for all systems services delivered under this Task Order. The contractor shall provide COTS manuals, supplemental data for COTS manuals, and documentation IAW best commercial practices (i.e. CD-ROM, etc.). This documentation shall include users' manuals, operators' manuals, maintenance manuals, and network and application interfaces if specified in the task order.

### 5.13 Enterprise Software Initiative

In situations where the purchase of new COTS software is needed to satisfy the requirements of a particular task order, the contractor shall use available existing enterprise licenses. If enterprise licenses are unavailable, then products will be obtained via the DoD Enterprise Software Initiative (ESI) Blanket Purchase Agreements (BPAs). If products are unavailable from ESI, then products will be acquired through the NETCENTS-2 Products contract. The updated listing of COTS software available from DoD ESI sources can be viewed on the web at http://www.esi.mil.

### 5.14 Software License Management

When required at the task order level, the contractor shall provide maintenance and support to control the entire asset life-cycle, from procurement to retirement, which includes applications, license agreements as well as software upgrades. The contractor shall provide asset inventory and services that track the financial aspects of an asset to include cost and depreciation, contract management, leases, maintenance agreements and service contracts. The contractor shall provide support summary information to include the general terms and conditions, benefits, strategic and tactical directions, license ordering information, internal billing process, pricing and deployment and support of the products included in the agreement. The contractor shall support common practices for ordering assets, tracking orders and assets, and tagging the assets. The contractor shall support application installation, operations, customer support, training, maintenance, sustainment and configuration control, to include the procurement of supporting software licenses.

### 5.15 Transition and Decommissioning Plans

The contractor shall create transition and decommissioning plans that accommodate all of the non-authoritative data sources (non-ADS) interfaces and ensure that necessary capabilities are delivered using approved ADSs.

### 5.16 Prototypes

The contractor shall develop prototypes as required in task orders. The contractor shall operate and maintain prototype applications, models and databases to determine optimal solutions for integration concepts and problems integral to the integration process. The contractor shall develop schedules and implementation plans with definable deliverables, including parallel operations where required, identification of technical approaches, and a description of anticipated prototype results.

### 5.17 Section 508 of the Rehabilitation Act

The Contractor shall meet the requirements of the Access Board's regulations at 36 CFR Part 1194, particularly 1194.22, which implements Section 508 of the Rehabilitation Act of 1973, as amended. Section 508 (as amended) of the Rehabilitation Act of 1973 (20 U.S.C. 794d) established comprehensive requirements to ensure: (1) Federal employees with disabilities are able to use information technology to do their jobs, and (2) members of the public with disabilities who are seeking information from Federal sources will be able to use information technology to access the information on an equal footing with people who do not have disabilities.

### 5.18 Performance of Services During Crisis Declared by the President of the United States, the Secretary of Defense, or Overseas Combatant Commander

The performance of these services may be considered mission essential during time of crisis. Should a crisis be declared by the Secretary of Defense, the TO CO or representative will verbally advise the contractor of the revised requirements, followed by written direction. When a crisis is declared, all services identified in this PWS are considered critical services during a crisis. The contractor shall continue providing service to ESC 24 hours a day until the crisis is over. The contractor shall ensure enough skilled personnel are available during a crisis for any operational emergency. A crisis management plan shall be submitted IAW A-TE-3, A04. The contractor will be notified by the Contracting Officer should a crisis be declared affecting needed Contractor support. Also, it must include the **Performance of Service During Crisis** language spelled out in AFI 63-124 paragraph 2.7.1. This requires the PWS to identify services determined essential during a crisis situation in accordance with DODI 3020.37. The statement is to be used is "***The FC/FD has determined that this requirement is/is not Mission Essential (M-E) in accordance with DoDI 3020.37." (NOTE: Remember only the FC/FD (not the MFT) can make this determination and read DoDI 3020.37 regarding the required plan if the contractor is determined mission essential.)***

### 5.19 Anthrax Information:

**IF APPLICABLE**, include the following statement: "In accordance with the Air Force Anthrax Vaccine Immunization Program (AVIP), 18 Jan 2007, any Mission Essential contractor personnel performing work in the CENTCOM AOR or Korea for greater than 15 consecutive days are required to obtain the Anthrax vaccination."

### 5.20 Electronic Ordering Process

***[This is a living document, future updates may require PWS tailoring.]***

Task orders will be procured using Requests for Proposals (RFPs) processed through a means specified at the time of task order procurement.

### 5.21 Incentives

***[Incentives should be used to encourage better quality performance and may be either positive, negative or a combination of both; however, they do not need to be present in every performance-based Task Order as an additional fee structure. In a fixed price Task Order, the incentives would be embodied in the pricing and the contractor could either maximize profit through effective performance or have payments reduced because of failure to meet the performance standard.***

***Positive Incentives - Actions to take if the work exceeds the standards;***

***Negative Incentives - Actions to take if work does not meet standards;***

***The definitions of standard performance, maximum positive and negative performance incentives, and the units of measurement should be documented here. They will vary from Task Order to Task Order and are subject to discussion during a source selection. It is necessary to balance value to the Government and meaningful incentives to the contractor. Incentives should correlate with results. Follow-up is necessary to ensure that desired results are realized, i.e., ensuring that incentives actually encourage good performance and discourage unsatisfactory performance.]***

## 6. SERVICES DELIVERY SUMMARY

***[Modify to fit the services being required of this Task Order. Make sure the services required have measurable outcomes.]***

| Performance Requirements | Performance Threshold | Monitoring Method |
|---|---|---|
| **APPLICATION AVAILABILITY** | | |
| Unscheduled application downtime | Customer meets application availability thresholds; Equal or fewer than 61.2 hours | QAE monthly review of system metrics |
| Unscheduled application downtime | Customer exceeds application availability thresholds; Equal or fewer than 26.2 hours | QAE monthly review of system metrics |
| Unscheduled application downtime | Customer exemplifies application availability thresholds; Equal or fewer than 4.4 hours | QAE monthly review of system metrics |
| Scheduled application downtime | Customer meets application availability thresholds; Equal or fewer than 200 hours | QAE monthly review of system metrics |
| Scheduled application downtime | Customer exceeds application availability thresholds; Equal or fewer than 50 hours | QAE monthly review of system metrics |

| Performance Requirements | Performance Threshold | Monitoring Method |
|---|---|---|
| Scheduled application downtime | Customer exemplifies application availability thresholds; Equal or fewer than 12 hours | QAE monthly review of system metrics |
| Mean Time To Restore (MTTR) | Time allowed for the system to be offline after application availability is interrupted. Mission-critical IT systems have a MTTR of two hours or fewer; non-mission-critical IT systems have a MTTR as short as five hours | QAE monthly review of system metrics |
| Recovery Time Objective (RTO) | The time it takes from the time of disaster to the time of service restoration and access by customers. Dependent on mission criticality | QAE monthly review of system metrics |
| Recovery Point Objective (RPO) | The amount of lost data that is acceptable after a disaster. Anywhere from zero to the point of the last backup of 24 hours | QAE monthly review of system metrics |
| User incidents | ( X affected users / Y total users) * 100 = % Application Availability; Maximum % effected dependent on mission criticality | QAE monthly review of system metrics |
| **APPLICATION PERFORMANCE** | | |
| Bandwidth utilization | Bandwidth utilization is kept to a minimum while not sacrificing application service performance; does not exceed X Mb, Gb | QAE monthly review of system metrics |
| Ports and protocols | Applications are using the port/protocol as specified by policy | QAE monthly review of system metrics |
| Computing requirements and resources (virtual environments) | Projected amount of computing resources and requirements is not exceeded; actual versus projected difference in computing resources (CPU, RAM, storage, etc.) acceptable | QAE monthly review of system metrics |
| User load/capacity | Services allow for the specified number of users required while not impacting system performance | QAE monthly review of system metrics |
| Data load | Job/process maximum load allowed; each job/process does not exceed X% utilization of CPU/RAM/IOP/etc | QAE monthly review of system metrics |
| Throughput | Amount of transactions per second permissible; applicable to service transactions or database transactions | QAE monthly review of system metrics |

| Performance Requirements | Performance Threshold | Monitoring Method |
|---|---|---|
| Response time | Average, maximum allowable response time for a user transaction; user transaction should not exceed X amount of seconds, minutes | QAE monthly review of system metrics |
| Degradation modes | Acceptable mode of operation when the system has been degraded in some manner | QAE monthly review of system metrics |
| Maximum bugs or defect rate | Expressed in terms of bugs/KLOC; categorized in terms of minor, significant, and critical; dependent on mission criticality | QAE monthly review of system metrics |
| Accuracy | Specify precision (resolution) and accuracy (known standard) that is required in the systems output | QAE monthly review of system metrics |
| **SYSTEM OPERATIONS & MAINTENANCE** | | |
| Sustainment activities | Legacy systems are sustained without periods of prolonged degradation | QAE monthly review of system metrics |
| Sustainment activities | Complex software problems are isolated and resolved | QAE monthly review of system metrics |
| Database administration | Maintain development and test environments and databases; operating system and software upgrades, patches, and hot fixes are applied | Random sampling, 100% inspection, periodic sampling |
| Performance tuning and development | Margin of improvement for application services; Y=after; X=before; (Y-X)/X=system improvement or degradation | QAE monthly review of system metrics |
| Establish individual User Accounts (including email) | # of business hours until completion from time of notification by Service Recipient; 8 hours, 80% of the time | Measure weekly and report monthly |
| Password Reset | # of minutes until completion from time of notification by Service Recipient; 30 minutes, 95% of the time | Measure weekly and report monthly |
| Delete User Accounts (including email) | # of business hours until completion from time of notification by Service Recipient; 1 day | Measure weekly and report monthly |
| Backup and Restore Requirements | Provider shall implement and maintain backup and restoration capabilities for all data, applications and component configurations; backup frequency – daily, weekly, monthly; retention period – dependent on mission criticality and policy | Measure weekly and report monthly |

| Performance Requirements | Performance Threshold | Monitoring Method |
|---|---|---|
| **SOFTWARE DESIGN, DEVELOPMENT & TESTING** | | |
| Software procurement analysis | Feasibility analysis, detailed analysis | 100% inspection |
| Software design | Output may be tailored for efficiency: revised modification list, updated design baseline, updated test plans, revised detailed analysis, verified requirements, revised implementation plan, and a list of documented constraints and risks | 100% inspection |
| Software coding design | Each modified software unit and database ('packing list'); test procedures and data for testing each software unit and database | 100% inspection |
| Software implementation | Output may be tailored for efficiency; Updated software and design documents, Updated test documents, recommended updates to impacted portions of the training materials, test readiness review report | 100% inspection |
| Software testing | Output may be tailored for efficiency; tested and fully integrated system, system test report, acceptance test readiness review report | 100% inspection |
| Software acceptance support | The output of this activity may be tailored and shall be at least one of the following; new system baseline, functional configuration audit report, acceptance test report | 100% inspection |
| Software delivery | Delivery plan (when directed), participation and documentation of installation event (mandatory) | 100% inspection |
| **QUALITY ASSURANCE** | | |
| Configuration management database updates and accuracy | Configuration management database updated with new systems or software with 2 duty days | QAE random checks |
| Configuration management database updates and accuracy | Configuration management database includes all systems and software and a 98% accuracy rate is maintained at all times | QAE random checks |
| IT systems inventory updates and accuracy | IT system inventories include all systems and software and a 98% accuracy rate is maintained | QAE random checks |
| Accuracy of software architecture drawings | More than 95% of all changes to architecture drawings updated within one week | QAE random checks |

| Performance Requirements | Performance Threshold | Monitoring Method |
|---|---|---|
| Change request rate | Change requests are increasing on a month-to-month basis | QAE random checks |
| Change management resolution time | The time it takes to initiate a request, address/resolve the request, and close out the request are kept to a minimum; dependent on mission criticality | QAE random checks |
| Configuration management | Configuration management practices are followed as prescribed by AF procedures to include version control, etc | QAE random checks |
| Change management | Change management practices are followed as prescribed by AF procedures | QAE random checks |
| Incident/Problem resolution | The number of identified problems should continue to decrease or not exceed a certain monthly threshold | QAE random checks |
| Software management | Between 95-98% of scheduled upgrades and/or maintenance are executed according to schedule | Event-driven and call-handling activity reports |
| Software management | For non-mission critical applications, between 80-90% of requests for unscheduled software maintenance are responded to within 48 hours | Event-driven and call-handling activity reports |
| Software management | For mission critical applications, 95-100% of requests are responded to within 2 hours | Event-driven and call-handling activity reports |
| Use of energy efficient equipment | 95% of new electronic equipment must meet agency environmental requirements as described by Energy Star, FEMP, or EPEAT guidelines | QAE monthly review of contractor metrics |
| Minimize energy consumption | Meet the energy reduction goal of 3% annually through FY 2015 or a 30% reduction by the end of FY 2015 | QAE monthly review of contractor metrics |
| Employees security clearances; control access badges; control limited access areas; maintain security of government facilities, classified data and material | Available 24/7/365 to respond within two hours to security incidents 100% of the time | QAE random checks and review of security incident information |
| **INFORMATION ASSURANCE** | | |
| System security compliance | Maintain C&A compliance IAW applicable DoD and AF policy and instruction, particularly DoD Instruction 8500.2 – Information Assurance | Random sampling, 100% inspection, periodic sampling |

| Performance Requirements | Performance Threshold | Monitoring Method |
|---|---|---|
| Application security compliance | Maintain application security compliance IAW applicable DoD and AF policy and instruction, particularly the Security Technical Implementation Guide (STIG) | Random sampling, 100% inspection, periodic sampling |
| Use Enterprise Information Technology Data Repository (EITDR) or Enterprise Mission Assurance Support Service (eMASS) to conduct virtual evaluation of systems security | Used to conduct virtual evaluations of a programs Security, Interoperability, Supportability, Sustainability, and Usability (SISSU) information, input is required into the EITDR or eMASS system 100% of the time | Random sampling, 100% inspection, periodic sampling |
| **TRAINING** | | |
| Training | Specify the required training time for normal users and power users to become productive at particular operations; dependent on mission | Random sampling, 100% inspection, periodic sampling |
| Training materials | Timely training materials are provided on time as required by a CDRL or contract requirement | Random sampling, 100% inspection, periodic sampling |
| Training materials | Quality training materials are provided to the customer that accurately reflect and correspond to processes and services | Random sampling, 100% inspection, periodic sampling |
| **HELP DESK SUPPORT** | | |
| Help desk support | Provide problem resolution for assigned calls; 100% of assigned calls have a problem resolution | Random sampling, 100% inspection |
| Customer assistance performance | Contractor propose industry best practices for speed to answer rate, true call abandonment rate, level 1 resolution rate, and call resolution rate, etc | QAE monthly review of contractor metrics and customer feedback |
| Customer Satisfaction | Contractor propose industry best practices for customer satisfaction surveys | QAE random review of customer surveys |
| Admin Changes (Access user ID, password reset) | 98% completed $\leq$ 1 business days (Changes done electronically) | QAE monthly review of contractor metrics |
| Average speed to answer calls | 80% answered <30 sec | QAE monthly review of call handling activity reports |
| Help desk Agent Utilization Rate | Rate should remain between 65% - 75% (Talk time + after call work time) | Totals and averages are usually reported monthly; both numerically (tabular data) and graphically |

| Performance Requirements | Performance Threshold | Monitoring Method |
|---|---|---|
| Abandoned Call Rate | <5% of calls abandoned | Totals and averages are usually reported monthly; both numerically (tabular data) and graphically |
| First Call Resolution | 65 % of problems resolved during initial call | Automated extraction from enterprise-class service desk toolset with focus on monthly average trending |
| Follow-on calls due to problem repeated after initial fix failed | 10% for the first two months with a 1% reduction per month until 5% is achieved | Service Provider provided system has capability to track and report out of compliance activities |
| Call Center Availability | 99.5% Availability | Service Provider provided system has capability to track and report out of compliance activities |

## 7. DATA DELIVERABLES

***[Define deliverables required for individual Task Orders. This section contains information on data requirements, such as reports or any of those items contained within a Contract Data Reports List (CDRL). Strive to minimize data requirements that require government approval and delivery. Only acquire data that are absolutely necessary. The usual rule of thumb is to limit data to those needed by the government to make a decision or to comply with a higher level requirement. Deliverables should relate directly to the Services Delivery Summary in Section 6. Detailed CDRL requirements and formats should be provided IAW DFAR 204.7105 on DD Form 1423-1, FEB 2001.]***

The Government requires all deliverables that include Scientific and Technical Information (STINFO), as determined by the Government, be properly marked IAW DoD Directive 5230.24 and AFI 61-204 prior to initial coordination or final delivery. Failure to mark deliverables as instructed by the Government will result in non-compliance and non-acceptance of the deliverable. The contractor shall include the proper markings on any deliverable deemed STINFO regardless of media type, stage of completeness, or method of distribution. Therefore, even draft documents containing STINFO and STINFO sent via e-mail require correct markings. Additionally, as required by individual Task/Delivery Orders, the contractor shall formally deliver as a CDRL all intellectual property, software, licensing, physical records, files, documents, working papers, and other data for which the Government shall treat as deliverable.

| Sequence Number | Data Item Description | Title |
|---|---|---|
| A001 | DI-ADMN-81249A | Conference Agenda |
| A002 | DI-ADMN-81250A | Conference Minutes |

| Sequence Number | Data Item Description | Title |
|---|---|---|
| A003 | DI-ADMN-81306 | Program Protection Implementation Plan (PPIP) |
| A004 | DI-ADMN-81308A | Conference Report |
| A005 | DI-ADMN-81373 | Presentation Material |
| A006 | DI-ADMN-81505 | Report, Record of Meeting/Minutes |
| A007 | DI-CMAN-80463C | Engineering Release Record (ERR) |
| A008 | DI-CMAN-80639C | Engineering Change Proposal (ECP) |
| A009 | DI-CMAN-80640C | Request for Deviation (RFD) |
| A010 | DI-CMAN-80642C | Notice of Revision (NOR) |
| A011 | DI-CMAN-80643C | Specification Change Notice (SCN) |
| A012 | DI-CMAN-80792A | Validation Report |
| A013 | DI-CMAN-80858B | Contractor's Configuration Management Plan |
| A014 | DI-CMAN-80874 | Configuration Data Lists (CDLS) |
| A015 | DI-CMAN-81022C | Configuration Audit Summary Report |
| A016 | DI-CMAN-81121 | Baseline Description Document |
| A017 | DI-EDRS-80410 | Engineering Documentation Information |
| A018 | DI-FACR-80810A | Test Facility Requirements Document (TFRD) |
| A019 | DI-ILSS-80481A | Source, Maintenance and Recoverability (SMR) Code Change Request |
| A020 | DI-ILSS-80812 | Logistic Technical Data User Profile |
| A021 | DI-ILSS-80813 | List of Logistic Technical Data Users |
| A022 | DI-ILSS-80872 | Training Materials |
| A023 | DI-ILSS-81070 | Training Program Development and Management Plan |
| A024 | DI-ILSS-81495 | Failure Mode Effects, and Criticality Analysis Report |
| A025 | DI-IPSC-80590B | Computer Program End Item Documentation |
| A026 | DI-IPSC-80942 | Computer Software System Document |
| A027 | DI-IPSC-81427A | Software Development Plan (SDP) |
| A028 | DI-IPSC-81428A | Software Installation Plan (SIP) |
| A029 | DI-IPSC-81429A | Software Transition Plan (STRP) |
| A030 | DI-IPSC-81430A | Operational Concept Description (OCD) |
| A031 | DI-IPSC-81431A | System/Subsystem Specification (SSS) |
| A032 | DI-IPSC-81432A | System/Subsystem Design Description (SSDD) |
| A033 | DI-IPSC-81433A | Software Requirements Specification (SRS) |
| A034 | DI-IPSC-81434A | Interface Requirements Specification (IRS) |
| A035 | DI-IPSC-81435A | Software Design Description (SDD) |
| A036 | DI-IPSC-81436A | Interface Design Description (IDD) |
| A037 | DI-IPSC-81437A | Database Design Description (DBDD) |
| A038 | DI-IPSC-81438A | Software Test Plan (STP) |
| A039 | DI-IPSC-81439A | Software Test Description (STD) |
| A040 | DI-IPSC-81440A | Software Test Report (STR) |
| A041 | DI-IPSC-81441A | Software Product Specification (SPS) |

| Sequence Number | Data Item Description | Title |
|---|---|---|
| A042 | DI-IPSC-81442A | Software Version Description (SVD) |
| A043 | DI-IPSC-81443A | Software User Manual (SUM) |
| A044 | DI-IPSC-81444A | Software Center Operator Manual (SCOM) |
| A045 | DI-IPSC-81445A | Software Input / Output Manual (SIOM) |
| A046 | DI-IPSC-81446A | Computer Operation Manual (COM) |
| A047 | DI-IPSC-81447A | Computer Programming Manual (CPM) |
| A048 | DI-IPSC-81448A | Firmware Support Manual (FSM) |
| A049 | DI-IPSC-81488 | Computer Software Product |
| A050 | DI-IPSC-81633 | Software Programmer's Guide |
| A051 | DI-IPSC-81756 | Software Documentation |
| A052 | DI-MCCR-80459 | Software Developmental Status Report (SDSR) |
| A053 | DI-MCCR-80491A | Computer Software Flowchart |
| A054 | DI-MCCR-80700 | Computer Software Product End Items |
| A055 | DI-MCCR-80902 | Software Development Summary Report |
| A056 | DI-MCCR-81344 | Design Specification |
| A057 | DI-MGMT-80061A | Engineering and Technical Services Accomplishment Report |
| A058 | DI-MGMT-80224B | Technical Directive Compliance Reports |
| A059 | DI-MGMT-80227 | Contractor's Progress, Status and Management Report |
| A060 | DI-MGMT-80269 | Status of Government Furnished Equipment (GFE) Report |
| A061 | DI-MGMT-80277 | Government Furnished Inspection Equipment Maintenance Report |
| A062 | DI-MGMT-80368A | Status Report |
| A063 | DI-MGMT-80389B | Receipt of Government Material Report |
| A064 | DI-MGMT-80408B | Request for Government Furnished Materiel |
| A065 | DI-MGMT-80469A | System Assessment Report (SAR) |
| A066 | DI-MGMT-80501 | Contractor's Corrective Action Plan |
| A067 | DI-MGMT-80507C | Project Planning Chart |
| A068 | DI-MGMT-80555A | Program Progress Report |
| A069 | DI-MGMT-80920 | List of Items Delivered During the Term of a Contract |
| A070 | DI-MGMT-81466A | Contract Performance Report (CPR) |
| A071 | DI-MGMT-81580 | Contractor's Standard Operating Procedures |
| A072 | DI-MGMT-81642 | Small Business Subcontractor Report |
| A073 | DI-MGMT-81739B | Software Resources Data Reporting: Initial Developer Report and Data Dictionary |
| A074 | DI-MGMT-81740A | Software Resources Data Reporting: Final Developer Report and Data Dictionary |
| A075 | DI-MGMT-81793 | Request Contract Change (RCC) Report |
| A076 | DI-MGMT-81797 | Program Management Plan |
| A077 | DI-MGMT-81808 | Contractor's Risk Management Plan |
| A078 | DI-MGMT-81809 | Risk Management Status Report |
| A079 | DI-MGMT-81834 | Contractor's Personnel Roster |

| Sequence Number | Data Item Description | Title |
|---|---|---|
| A080 | DI-MGMT-81842 | Vulnerability Scan Compliance (VSC) Report |
| A081 | DI-MGMT-81843 | Information Assurance (IA) Test Report |
| A082 | DI-MGMT-81844 | Information Assurance (IA) Test Plan |
| A083 | DI-MGMT-81845 | Information Assurance (IA) Design Review Information Package (DRIP) |
| A084 | DI-MISC-80392 | Operating Instructions |
| A085 | DI-MISC-80393A | Master Document List (MDL) |
| A086 | DI-MISC-80394 | Disaster Preparedness Exercise Evaluation Report |
| A087 | DI-MISC-80564 | Vulnerability Analysis Report |
| A088 | DI-MISC-80678 | Certification/Data Report |
| A089 | DI-MISC-80711A | Scientific and Technical Reports |
| A090 | DI-MISC-80734 | Technical Data Assessment |
| A091 | DI-MISC-80749 | Specifications and Standards Usage Report |
| A092 | DI-MISC-80750 | Technical Data Package Review Report |
| A093 | DI-MISC-80751 | English Language Test Design Document (ELTD) |
| A094 | DI-MISC-81350 | Trusted Computing Base Verification Report |
| A095 | DI-MISC-81356A | Certificate of Compliance |
| A096 | DI-MISC-81418 | Operating Procedures Manual |
| A097 | DI-MISC-81479 | Ozone Depleting Substances (ODS) Plan |
| A098 | DI-MISC-81612B | Research and Development (R&D) Project Summary |
| A099 | DI-MISC-81627 | System Deficiency Report (SDR) Data |
| A100 | DI-MISC-81807 | Software/Firmware Change Request |
| A101 | DI-NUOR-81412 | Software Certification Plan (SCP) |
| A102 | DI-QCIC-80125B | Government Industry Data Exchange Program (GIDEP) Alert/Safe-Alert Report |
| A103 | DI-QCIC-80126B | Government Industry Data Exchange Program (GIDEP) Alert Response |
| A104 | DI-QCIC-80127A | GIDEP Annual Progress Report |
| A105 | DI-QCIC-80736 | Quality Deficiency Report |
| A106 | DI-QCIC-81009 | Technical Data Package Quality Control Program Plan |
| A107 | DI-QCIC-81013 | Technical Data Package Validation Report |
| A108 | DI-QCIC-81187 | Quality Assessment Report |
| A109 | DI-QCIC-81200 | Quality Inspection Test, Demonstration, and Evaluation Report |
| A110 | DI-QCIC-81379 | Quality System Plan |
| A111 | DI-QCIC-81794 | Quality Assurance Program Plan |
| A112 | DI-QCIC-81795 | Software Quality Assurance Report |
| A113 | DI-RELI-80254 | Corrective Action Plan |
| A114 | DI-RELI-80255 | Failure Summary and Analysis Report |
| A115 | DI-RELI-80685 | Critical Items List |
| A116 | DI-RELI-80807 | Failure Data and Traceability Record |
| A117 | DI-SAFT-80101B | System Safety Hazard Analysis Report (SSHA) |
| A118 | DI-SAFT-80102B | Safety Assessment Report (SAR) |

| Sequence Number | Data Item Description | Title |
|---|---|---|
| A119 | DI-SAFT-80104B | Waiver or Deviation System Safety Report (WDSSR) |
| A120 | DI-SAFT-80105B | System Safety Program Progress Report (SSPPR) |
| A121 | DI-SAFT-81563 | Accident/Incident Report |
| A122 | DI-SAFT-81626 | System Safety Program Plan (SSPP) |
| A123 | DI-SESS-81001D | Conceptual Design Drawings/Models |
| A124 | DI-SESS-81002E | Developmental Design Drawings/Models and Associated Lists |
| A125 | DI-SESS-81785 | Systems Engineering Management Plan (SEMP) |
| A126 | DI-TMSS-80007 | Test Program Manual |
| A127 | DI-TMSS-80527C | Commercial Off-The-Shelf (COTS) Manuals and Associated Supplemental Data |
| A128 | DI-TMSS-81815 | Commercial Off-The-Shelf (COTS) Manuals |
| A129 | DI-TMSS-81816 | Commercial Off-The-Shelf (COTS) Manual Supplemental Data |
| A130 | DI-TMSS-81817 | Technical Manual Quality Assurance (TMQA) Program Plan |
| A131 | DI-TMSS-81818 | Technical Manual Validation Plan |
| A132 | DI-TMSS-81819A | Technical Manual Validation Certificate |
| A133 | DI-TMSS-81820 | Technical Manual Verification Discrepancy/Disposition Record |
| A134 | DI-TMSS-81821 | Technical Manual Verification Incorporation Certificate |

## 8. APPLICABLE STANDARDS AND REFERENCES

***[Tailor the list as needed for individual Task Orders requirements. The list is not all-inclusive and the most current version of the document at the time of task order issuance will take precedence. Web links are provided wherever possible.]***

| Documentation | URL | Description |
|---|---|---|
| **ENTERPRISE STRATEGY** | | |
| DoD CIO Net-Centric Data Strategy | http://www.defenselink.mil/cio-nii/docs/Net-Centric-Data-Strategy-2003-05-092.pdf | This document describes the Net-Centric Data Strategy for the Department of Defense (DoD), including DoD intelligence agencies and functions. It describes a vision for a net-centric environment and the data goals for achieving that vision. It defines approaches and actions that DoD personnel will have to take as users—whether in a role as consumers and producers of data or as system and application developers. |
| DoD CIO Net-Centric Services Strategy | http://cio-nii.defense.gov/docs/Services_Strategy.pdf | The DoD Net-Centric Services Strategy (NCSS) [R1313] builds upon the DoD Net-Centric Data Strategy's (May 2003) goals of making data assets visible, accessible, and understandable. The NCSS establishes services as the preferred means by which data producers and capability providers can make their data assets and capabilities available across the DoD and beyond. It also establishes services as the preferred means by which consumers can access and use these data assets and capabilities. |

| Documentation | URL | Description |
|---|---|---|
| DoD Discovery Metadata Specification (DDMS) | http://metadata.dod.mil/mdr/irs/DDMS/ | Visibility, accessibility, and understandability are the high priority goals of the DoD Net-Centric Data Strategy. Of these goals, visibility and discovery are intimately linked. Visibility of a resource is, in a practical sense, useless, if the resource is not easily discoverable. With the express purpose of supporting the visibility goal of the DoD Net-Centric Data Strategy, the DDMS specifies a set of information fields that are to be used to describe any data or service asset, i.e., resource, that is to be made discoverable to the Enterprise, and it serves as a reference for developers, architects, and engineers by laying a foundation for Discovery Services. |
| CJCSI 6211.02D, Defense Information Systems Network Responsibilities | http://www.dtic.mil/cjcs_directives/cdata/unlimit/6211_02.pdf | This instruction establishes policy and responsibilities for the connection of information systems (ISs) (e.g., applications, enclaves, or outsourced processes) and unified capabilities (UC) products to the DISN provided transport (including data, voice, and video) and access to information services transmitted over the DISN (including data, voice, video, and cross-domain). |
| CJCSI 6212.01E, Interoperability and Supportability of Information Technology and National Security Systems | http://www.dtic.mil/cjcs_directives/cdata/unlimit/6212_01.pdf | Establishes policies and procedures for developing, coordinating, reviewing, and approving Information Technology (IT) and National Security System (NSS) Interoperability and Supportability (I&S) needs. Establishes procedures to perform I&S Certification of Joint Capabilities Integration and Development System (JCIDS) Acquisition Category (ACAT) programs and systems. Defines the five elements of the Net-Ready Key Performance Parameter (NR-KPP). Provides guidance for NR-KPP development and assessment. |
| DoDI 4630.8, Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS) | http://www.dtic.mil/whs/directives/corres/pdf/463008p.pdf | Implements a capability-focused, effects-based approach to advance IT and NSS interoperability and supportability throughout the Department of Defense (DoD). This approach incorporates both materiel (acquisition or procurement) and non-materiel (doctrine, organizational, training, leadership and education, personnel, and facilities) aspects to ensure life-cycle interoperability and supportability of IT and NSS throughout the DoD. Implements the Net-Ready Key Performance Parameter (NR-KPP) to assess net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. The NR-KPP replaces the Interoperability KPP and incorporates net-centric concepts for achieving IT and NSS interoperability and supportability. |
| Netcentric Enterprise Solutions for Interoperability (NESI) | http://nesipublic.spawar.navy.mil/ | NESI is a body of architectural and engineering knowledge that guides the design, implementation, maintenance, evolution, and use of the Information Technology (IT) portion of net-centric solutions for defense application. |
| **ENTERPRISE ARCHITECTURE** | | |

| Documentation | URL | Description |
|---|---|---|
| Department of Defense Architecture Framework (DoDAF) Ver2.02 Aug 2010 | http://cio-nii.defense.gov/sites/dodaf20/index.html | The Department of Defense Architecture Framework (DoDAF), Version 2.0 is the overarching, comprehensive framework and conceptual model enabling the development of architectures to facilitate the ability of Department of Defense (DoD) managers at all levels to make key decisions more effectively through organized information sharing across the Department, Joint Capability Areas (JCAs), Mission, Component, and Program boundaries. The DoDAF serves as one of the principal pillars supporting the DoD Chief Information Officer (CIO) in his responsibilities for development and maintenance of architectures required under the Clinger-Cohen Act. DoDAF is prescribed for the use and development of Architectural Descriptions in the Department. It also provides extensive guidance on the development of architectures supporting the adoption and execution of Net-centric services within the Department. |
| AFI33-401, Implementing Air Force Architectures | http://www.af.mil/shared/media/epubs/AFI33-401.pdf | This Air Force Instruction (AFI) implements Air Force Policy Directive (AFPD) 33-4, Enterprise Architecting. This instruction describes the federation of Air Force architectures and its concept for federated architecture development, its associated business rules, governance, and the roles and responsibilities for appropriate Air Force organizations. |
| **SYSTEMS ENGINEERING** | | |
| Air Force Program Executive Office (AFPEO) Business Enterprise Systems (BES) Systems Engineering Process | https://org.eis.afmc.af.mil/sites/754elsg/ES/HIJG/SEP/default.aspx | The Systems Engineering Process is a life cycle management and systems engineering process based on the Defense Acquisition, Technology, and Logistics Life Cycle Management System as tailored for Information Technology Systems and the Capability Maturity Model Integrated. It provides common plans, procedures, checklists, forms, and templates that support system life cycle management and systems engineering processes. |
| AFI 63-1201, Life Cycle Systems Engineering | http://www.e-publishing.af.mil/shared/media/epubs/afi63-1201.pdf | It identifies elements of Air Force systems engineering (SE) practice and management required to provide and sustain, in a timely manner, cost-effective products and systems that are operationally safe, suitable, and effective. |
| DoD Open Technology Development Guidebook | http://www.acq.osd.mil/jctd/articles/OTDRoadmapFinal.pdf | This roadmap outlines a plan to implement Open Technology Development practices, policies and procedures within the DoD. |
| Industry Best Practices in Achieving Service Oriented Architecture (SOA) | http://www.sei.cmu.edu/library/assets/soabest.pdf | This document was developed under the Net-Centric Operations Industry Forum charter to provide industry advisory services to the Department of Defense (DoD), Chief Information Officer (CIO). It presents a list of industry best practices in achieving Service Oriented Architecture (SOA). |
| Federal Desktop Core Configuration (FDCC) | http://nvd.nist.gov/fdcc/index.cfm | The United States Government Configuration Baseline (USGCB) is a Federal government-wide initiative that provides guidance to agencies on what should be done to improve and maintain an effective configuration settings focusing primarily on security. The USGCB baseline evolved from the Federal Desktop Core Configuration mandate. |
| **INFORMATION ASSURANCE** | | |

| Documentation | URL | Description |
|---|---|---|
| ICD 503, IT Systems Security, Risk Management, Certification and Accreditation | http://www.dni.gov/electronic_reading_room/ICD_503.pdf | This Intelligence Community Directive (ICD) establishes Intelligence Community (IC) policy for information technology systems security risk management, certification and accreditation. This ICD focuses on a more holistic and strategic process for the risk management of information technology systems, and on processes and procedures designed to develop trust across the intelligence community information technology enterprise through the use of common standards and reciprocally accepted certification and accreditation decisions. |
| DoDD 8500.01E Information Assurance (IA) | http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf | Establishes policy and assigns responsibilities to achieve Department of Defense (DoD) Information Assurance (IA) through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network centric warfare. |
| DoDI 8500.2, Information Assurance (IA) Implementation | http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf | Implements policy, assigns responsibilities, and prescribes procedures for applying integrated, layered protection of the DoD information systems and networks under DoD Directive 8500.01E, "Information Assurance." |
| Security Technical Implementation Guides (STIGs) | http://iase.disa.mil/stigs/stig/index.html | The Security Technical Implementation Guides (STIGs) and the NSA Guides are the configuration standards for DOD IA and IA-enabled devices/systems. The STIGs contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack. |
| DoD 8570.01, Information Assurance Training, Certification, and Workforce Management | http://www.dtic.mil/whs/directives/corres/pdf/857001p.pdf | Establishes policy and assigns responsibilities for Department of Defense (DoD) Information Assurance (IA) training, certification, and workforce management. |
| DoD 8570.01-M, Information Assurance Workforce Improvement Program | http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf | Provides guidance for the identification and categorization of positions and certification of personnel conducting Information Assurance (IA) functions within the DoD workforce supporting the DoD Global Information Grid (GIG) per DoD Instruction 8500.2. The DoD IA Workforce includes, but is not limited to, all individuals performing any of the IA functions described in this Manual. Additional chapters focusing on personnel performing specialized IA functions including certification and accreditation (C&A) and vulnerability assessment will be published as changes to this Manual. |
| AFI 33-200, Information Assurance | http://www.e-publishing.af.mil/shared/media/epubs/AFI33-200.pdf | This AFI provides general direction for implementation of IA and management of IA programs according to AFPD 33-2. Compliance ensures appropriate measures are taken to ensure the availability, integrity, and confidentiality of Air Force ISs and the information they process. |
| DoDI 8520.02 Public Key Infrastructure (PKI) and Public Key (PK) Enabling | http://www.dtic.mil/whs/directives/corres/pdf/852002p.pdf | This instruction establishes and implements policy, assign responsibilities, and prescribe procedures for developing and implementing a DoD-wide PKI and enhancing the security of DoD information systems by enabling these systems to use PKI for authentication, digital signatures, and encryption. |
| **INFORMATION TECHNOLOGY STANDARDS** | | |

| Documentation | URL | Description |
|---|---|---|
| Federal Information Processing Standards (FIPS) | http://www.itl.nist.gov/fipspubs/ | Under the Information Technology Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards and guidelines that are developed by the National Institute of Standards and Technology (NIST) for Federal computer systems. These standards and guidelines are issued by NIST as Federal Information Processing Standards (FIPS) for use government-wide. NIST develops FIPS when there are compelling Federal government requirements such as for security and interoperability and there are no acceptable industry standards or solutions. |
| Info-structure Technology Reference Model (i-TRM) | https://cs.eis.af.mil/a6/itrm/default.aspx | The i-TRM is the Air Force's authoritative source for Communications and Information (C&I) products, computer configurations, platform and service profiles, technical solutions, and standards (presented as standards profiles). |
| National Institute for Standards and Technology (NIST) | http://www.nist.gov/information-technology-portal.cfm | Advancing the state-of-the-art in IT in such applications as cyber security and biometrics, the National Institute of Standards and Technology accelerates the development and deployment of systems that are reliable, usable, interoperable, and secure; advances measurement science through innovations in mathematics, statistics, and computer science; and conducts research to develop the measurements and standards infrastructure for emerging information technologies and applications. |
| International Standards Organization (ISO) | http://www.iso.org/iso/home.html | ISO is the world's largest developer and publisher of International Standards. ISO is a network of the national standards institutes of 162 countries, one member per country, with a Central Secretariat in Geneva, Switzerland, that coordinates the system. ISO is a non-governmental organization that forms a bridge between the public and private sectors. On the one hand, many of its member institutes are part of the governmental structure of their countries, or are mandated by their government. On the other hand, other members have their roots uniquely in the private sector, having been set up by national partnerships of industry associations. Therefore, ISO enables a consensus to be reached on solutions that meet both the requirements of business and the broader needs of society. |
| American National Standards Institute (ANSI) | http://www.ansi.org/ | The Institute oversees the creation, promulgation and use of thousands of norms and guidelines that directly impact businesses in nearly every sector. ANSI is actively engaged in accrediting programs that assess conformance to standards – including globally-recognized cross-sector programs such as the ISO 9000 (quality) and ISO 14000 (environmental) management systems. |
| International Committee for Information Technology Standards | http://www.incits.org/ | INCITS is the primary U.S. focus of standardization in the field of Information and Communications Technologies (ICT), encompassing storage, processing, transfer, display, management, organization, and retrieval of information. As such, INCITS also serves as ANSI's Technical Advisory Group for ISO/IEC Joint Technical Committee 1. JTC 1 is responsible for International standardization in the field of Information Technology. |
| Institute of Electrical and Electronics Engineers (IEEE) | http://www.ieee.org/ | IEEE is the world's largest professional association dedicated to advancing technological innovation and excellence for the benefit of humanity. IEEE and its members inspire a global community through IEEE's highly cited publications, conferences, technology standards, and professional and educational activities. |

| Documentation | URL | Description |
|---|---|---|
| National Security Agency/The Common Criteria Evaluation/NIST and Validation Scheme | http://www.niap-ccevs.org/ | The National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) have established a program under the National Information Assurance Partnership (NIAP) to evaluate IT product conformance to international standards. The program, officially known as the NIAP Common Criteria Evaluation and Validation Scheme for IT Security (CCEVS) is a partnership between the public and private sectors. This program is being implemented to help consumers select commercial off-the-shelf information technology (IT) products that meet their security requirements and to help manufacturers of those products gain acceptance in the global marketplace. |
| Data Interchange Standards Association (DISA) | http://www.disa.org/ | The Data Interchange Standards Association (DISA) advances the foundation of electronic trade and commerce by supporting and promoting standards used for business-to-business data exchange. Providing administrative and technical support to the Accredited Standards Committee (ASC) X12, DISA helps individuals and organizations improve business processes, reduce costs, increase productivity and take advantage of new opportunities. |
| **QUALITY ASSURANCE** | | |
| AFPD 33-3, Information Management | http://www.e-publishing.af.mil/shared/media/epubs/AFPD33-3.pdf | This policy directive establishes Air Force policy for the management of information assets (all forms of data and content), across all AF information sources, as both a strategic resource and corporate asset supporting the warfighter during mission and support operations. |
| AFMAN 33-363, Management of Records | http://www.e-publishing.af.mil/shared/media/epubs/AFMAN33-363.pdf | This manual implements DoDD 5015.2, *DoD Records Management Program*, and Air Force Policy Directive (AFPD) 33-3, *Information Management*. It establishes the requirement to use the Air Force Records Information Management System (AFRIMS); establishes guidelines for managing all records (regardless of media); and defines methods and the format for record storage, file procedures, converting paper records to other media or vice versa, and outlines the minimum to comply with records management legal and policy requirements. |
| AFI 33-364, Records Disposition – Procedures and Responsibilities | http://www.e-publishing.af.mil/shared/media/epubs/AFI33-364.pdf | This instruction implements Air Force Policy Directive (AFPD) 33-3, *Information Management,* by listing program objectives and responsibilities, guiding personnel in disposing of special types of records, retiring or transferring records using staging areas, and retrieving information from inactive records. |
| DoDD 5230.24, Distribution Statements on Technical Documents | http://www.dtic.mil/whs/directives/corres/pdf/523024p.pdf | This Directive updates policies and procedures for marking technical documents, including production, engineering, and logistics information, to denote the extent to which they are available for distribution, release, and dissemination without additional approvals or authorizations. |
| AFI 61-204, Disseminating Scientific and Technical Information | http://www.e-publishing.af.mil/shared/media/epubs/afi61-204.pdf | This instruction updates the procedures for identifying export-controlled technical data and releasing export-controlled technical data to certified recipients and clarifies the use of the Militarily Critical Technologies List. It establishes procedures for the disposal of technical documents. |
| AFI 33-114, Software Management | http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA404975 | It identifies responsibilities for management of commercial off-the-shelf (COTS) and Air Force-unique software acquired by the Air Force. It includes policy and management structure for establishing and managing Air Force COTS software licenses and ensuring compliance with The Copyright Act and E.O. 13103. |

| Documentation | URL | Description |
|---|---|---|
| DoDD 5205.02, Operations Security (OPSEC) Program | http://www.fas.org/irp/doddir/dod/d5205_02.pdf | Underscores the importance of OPSEC and how it is integrated as a core military capability within Information Operations (IO) that must be followed in daily application of military operations. |
| AFI 10-701, Operations Security (OPSEC) | http://www.fas.org/irp/doddir/usaf/afi10-701.pdf | This publication provides guidance for all Air Force personnel (military and civilian) and supporting contractors in implementing, maintaining and executing OPSEC programs. It describes the OPSEC process and discusses integration of OPSEC into Air Force plans, operations and support activities. |
| Air Force Anthrax Vaccine Immunization Program (AVIP) | http://www.vaccines.mil/documents/1012AirForceImplementation.pdf | |
| DoD Manual 5200.01, DoD Information Security Program: Overview, Classification, and Declassification, V1-V4 | http://www.dtic.mil/whs/directives/corres/pdf/520001_vol1.pdf | The purpose of this manual is to implement policy, assign responsibilities, and provide procedures for the designation, marking, protection, and dissemination of controlled unclassified information (CUI) and classified information, including information categorized as collateral, sensitive compartmented information (SCI), and Special Access Program (SAP). |
| DoD 5220.22-M, National Industrial Security Program Operating Manual | http://www.dss.mil/documents/odaa/nispom2006-5220.pdf | This Manual is issued in accordance with the National Industrial Security Program (NISP). It prescribes the requirements, restrictions, and other safeguards to prevent unauthorized disclosure of classified information. The Manual controls the authorized disclosure of classified information released by U.S. Government Executive Branch Departments and Agencies to their contractors. It also prescribes the procedures, requirements, restrictions, and other safeguards to protect special classes of classified information, including Restricted Data (RD), Formerly Restricted Data (FRD), intelligence sources and methods information, Sensitive Compartmented Information (SCI), and Special Access Program (SAP) information. These procedures are applicable to licensees, grantees, and certificate holders to the extent legally and practically possible within the constraints of applicable law and the Code of Federal Regulations. |
| DoDI 2000.16, Antiterrorism Standards | http://www.dtic.mil/whs/directives/corres/pdf/200016p.pdf | Updates policy implementation, responsibilities, and the antiterrorism (AT) standards. This update reorganizes AT standards according to the minimum required elements for an AT program: risk management, planning, training and exercises, resource application, and comprehensive program review. |
| DoD 5400.7-R, Freedom of Information Act Program | http://www.dtic.mil/whs/directives/corres/pdf/540007r.pdf | This Regulation provides policies and procedures for the DoD implementation of the Freedom of Information Act (5 U.S.C. 552, as amended) and DoD Directive 5400.7, and promotes uniformity in the DoD Freedom of Information Act (FOIA) Program. |
| Section 508 of the Rehabilitation Act of 1973 | http://www.access-board.gov/sec508/guide/act.htm | On August 7, 1998, President Clinton signed into law the Rehabilitation Act Amendments of 1998 which covers access to federally funded programs and services. The law strengthens section 508 of the Rehabilitation Act and requires access to electronic and information technology provided by the Federal government. The law applies to all Federal agencies when they develop, procure, maintain, or use electronic and information technology. Federal agencies must ensure that this technology is accessible to employees and members of the public with disabilities to the extent it does not pose an "undue burden." Section 508 speaks to various means for disseminating information, including computers, software, and electronic office equipment. It applies to, but is not solely focused on, Federal pages on the Internet or the World Wide Web. |

| Documentation | URL | Description |
|---|---|---|
| DoDI 3020.37, Continuation of Essential DoD Contractor Services During Crises | http://www.afsc.army.mil/gc/files/i302037.pdf | This Instruction implements DoD policy, assigns responsibilities, and prescribes procedures, in accordance with references (a) and (b), to provide reasonable assurance of the continuation of essential services provided by DoD contractors, including services provided to Foreign Military Sales (FMS) customers, during crisis situations. |